Per realizzare la scansione completa e risolvere le vulnerabilità critiche indicate, procederemo come segue:

Fase 1: Scansione Iniziale

1. **Effettuare la scansione** sulla macchina Metasploitable con Nessus, ottenendo i risultati iniziali e identificando le vulnerabilità critiche.
2. **Documentare i risultati** con un report PDF (ScansioneInizio.pdf) che include il grafico delle vulnerabilità e i dettagli delle vulnerabilità critiche selezionate:
    - NFS Exported Share Information Disclosure
    - rexecd Service Detection
    - VNC Server 'password' Password
    - Bind Shell Backdoor Detection

Fase 2: Implementazione delle Azioni di Rimedio

Per ciascuna vulnerabilità critica identificata, implementeremo le seguenti azioni di rimedio:

1. **NFS Exported Share Information Disclosure**:
    - **Descrizione**: Il servizio NFS esporta condivisioni senza restrizioni adeguate.
    - **Rimedio**: Configurare le esportazioni NFS per limitare gli accessi solo ai client autorizzati. Modificare il file `/etc/exports` come segue:

      ```
      bash
      /path/to/share
      192.168.1.0/24(rw,sync,no_root_squash,no_subtree_check)
      ```

      Dove `192.168.1.0/24` rappresenta la subnet autorizzata.

2. **rexecd Service Detection**:
    - **Descrizione**: Il servizio `rexecd` è attivo e potrebbe essere sfruttato da attaccanti.
    - **Rimedio**: Disabilitare il servizio `rexecd` se non necessario. Eseguire i seguenti comandi:

      ```
      bash
      sudo systemctl stop rexecd
      sudo systemctl disable rexecd
      ```

3. **VNC Server 'password' Password**:
    - **Descrizione**: Il server VNC è configurato con una password debole.
    - **Rimedio**: Cambiare la password del server VNC con una password forte. Eseguire i seguenti comandi:

      ```
      bash
      vncpasswd
      ```

      Seguire le istruzioni per impostare una nuova password.

4. **Bind Shell Backdoor Detection**:
    - **Descrizione**: È stata rilevata una backdoor Bind Shell attiva.
    - **Rimedio**: Identificare e rimuovere la backdoor. Eseguire i seguenti comandi per identificare i processi sospetti:

```
bash
netstat -antp
```

Terminare i processi non autorizzati e rimuovere i file associati. Configurare il firewall per bloccare le connessioni non autorizzate.

5. **Regola Firewall (opzionale)**:
   - **Descrizione**: Implementare una regola firewall per proteggere ulteriormente il sistema.
   - **Rimedio**: Aggiungere una regola firewall per bloccare l'accesso alle porte vulnerabili da indirizzi IP non autorizzati. Eseguire i seguenti comandi:

```
bash
sudo ufw allow from 192.168.1.0/24 to any port 22
sudo ufw enable
```

Fase 3: Scansione Finale

1. **Eseguire una nuova scansione** con Nessus sulla macchina Metasploitable dopo aver implementato le azioni di rimedio.
2. **Documentare i risultati** della scansione finale in un report PDF (ScansioneFine.pdf) che evidenzia la risoluzione delle vulnerabilità.

Esempio di Report Unico (PDF)

Combineremo tutte le informazioni in un unico report PDF, diviso in tre sezioni principali:

1. **Scansione Iniziale**: Risultati e grafico delle vulnerabilità.
2. **Azioni di Rimedio**: Screenshot e spiegazione dei passaggi per la remediation.
3. **Scansione Finale**: Risultati e grafico delle vulnerabilità dopo le modifiche.

Esempio di Contenuto del Report Unico

```
plaintext
# Vulnerability Assessment Report: Metasploitable

## 1. Scansione Iniziale
### Risultati
| Severity | Score | Vulnerability Name                          |
|----------|-------|---------------------------------------------|
| Critical | 10.0  | NFS Exported Share Information Disclosure |
| Critical | 10.0  | rexecd Service Detection                    |
| Critical | 10.0  | VNC Server 'password' Password              |
| Critical | 9.8   | Bind Shell Backdoor Detection               |

### Grafico delle Vulnerabilità
![Vulnerability Graph](scansione_inizio_grafico.png)

## 2. Azioni di Rimedio
### NFS Exported Share Information Disclosure
- **Descrizione**: Il servizio NFS esporta condivisioni senza restrizioni
adeguate.
- **Rimedio**: Configurare `/etc/exports` per limitare l'accesso.
```plaintext
/path/to/share 192.168.1.0/24(rw,sync,no_root_squash,no_subtree_check)
```
```

- **Screenshot**:

rexecd Service Detection

- **Descrizione**: Il servizio `rexecd` è attivo e potrebbe essere sfruttato.
- **Rimedio**: Disabilitare il servizio `rexecd`.

```
plaintext
sudo systemctl stop rexecd
sudo systemctl disable rexecd
```

- **Screenshot**:

VNC Server 'password' Password

- **Descrizione**: Il server VNC è configurato con una password debole.
- **Rimedio**: Cambiare la password del server VNC.

```
plaintext
vncpasswd
```

- **Screenshot**:

Bind Shell Backdoor Detection

- **Descrizione**: È stata rilevata una backdoor Bind Shell attiva.
- **Rimedio**: Identificare e rimuovere la backdoor. Bloccare le connessioni non autorizzate.

```
plaintext
netstat -antp
sudo ufw allow from 192.168.1.0/24 to any port 22
sudo ufw enable
```

- **Screenshot**:

3. Scansione Finale

Risultati

Severity	Score	Vulnerability Name
Critical	10.0	NFS Exported Share Information Disclosure (Risolved)
Critical	10.0	rexecd Service Detection (Risolved)
Critical	10.0	VNC Server 'password' Password (Risolved)
Critical	9.8	Bind Shell Backdoor Detection (Risolved)

Grafico delle Vulnerabilità

```
markdown

### Passaggi per Creare il Report PDF
```

1. **Utilizzare un editor di testo** come Microsoft Word o Google Docs per compilare i contenuti.
2. **Inserire screenshot** e grafici come immagini nei punti appropriati del report.
3. **Esportare il documento** in formato PDF.

Questo approccio garantisce una documentazione completa e chiara delle vulnerabilità rilevate, delle azioni di rimedio implementate e dei risultati ottenuti dopo la mitigazione.